July 7, 2023

Overall rating: Critical

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of multiple Cisco vulnerabilities. There are numerous vulnerabilities, impacting multiple Cisco applications and devices detailed in the Cisco references below, VRM recommends reviewing the notifications and CVEs detailing the vulnerabilities, mitigations, and links to updates for your organizational systems.

Technical Details

Application	Impact	Vulnerability	Affected Products	Risk	CVE
Cisco Expressway Series and Cisco TelePresence Video Communication Server	May allow an authenticated attacker with Administrator-level read-only credentials to elevate their privileges to Administrator with read-write credentials on an affected system.	Privilege Escalation	These vulnerabilities affect Cisco Expressway Series and Cisco TelePresence VCS. The vulnerability described in CVE-2023-20192 only affects Cisco Expressway Series and Cisco TelePresence VCS if they are running a vulnerable release and have granted CLI access to a read-only administrator of the system.	CRITICAL	CVE-2023-20105 CVE-2023-20192
Cisco Unified Communications	May allow an unauthenticated, remote attacker to cause a	Denial of Service (DoS)	This vulnerability affects Cisco Unified CM IM&P.	HIGH	CVE-2023-20108

Manager IM & Presence Service	temporary service outage for all Cisco Unified CM IM&P users who are attempting to authenticate to the service, resulting in a denial of service (DoS) condition.				
Cisco Duo Authentication Proxy	May allow an authenticated, remote attacker to view sensitive information in clear text on an affected system.	Information Disclosure	This vulnerability affects Cisco Duo Authentication Proxy.	MEDIUM	CVE-2023-20207
Cisco Webex Meetings	May allow a remote attacker to conduct stored cross-site scripting (XSS) or cross-site request forgery (CSRF) attacks.	Cross-Site Scripting (XSS) and Cross-Site Request Forgery (CSRF)	These vulnerabilities affect Cisco Webex Meetings, which is cloud based.	MEDIUM	CVE-2023-20133 CVE-2023-20180
Cisco BroadWorks	May allow an authenticated, local attacker to elevate privileges to the root user on an affected device.	Privilege Escalation	This vulnerability affects the following Cisco products with the default configuration: • BroadWorks Application Delivery Platform • BroadWorks Application Server • BroadWorks Database Server • BroadWorks Database	MEDIUM	CVE-2023-20210

			Troubleshooting Server • BroadWorks Execution Server • BroadWorks Media Server • BroadWorks Messaging Server • BroadWorks Network Database Server • BroadWorks Network Function Manager • BroadWorks Network Server • BroadWorks Profile Server • BroadWorks Service Control Function Server • BroadWorks Sharing Server • BroadWorks Video Server • BroadWorks WebRTC Server • BroadWorks Xtended Services Platform		
Cisco Secure Email Gateway, Cisco Secure Email and Web Manager, and Cisco Secure Web Appliance	May allow a remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface.	Cross-Site Scripting (XSS)	• Secure Email and Web Manager, both virtual and hardware appliances • Secure Web Appliance, both virtual and hardware appliances	MEDIUM	CVE-2023-20028 CVE-2023-20119 CVE-2023-20120

Cisco Duo Authentication for macOS and Duo Authentication for Windows Logon	May allow an unauthenticated, physical attacker to replay valid user session credentials and gain unauthorized access to an affected macOS or Windows device.	Credentials Replay	• Duo Two-Factor Authentication for macOS • Duo Authentication for Windows Logon and RDP	MEDIUM	CVE-2023-20123
Cisco Duo Two-Factor Authentication for macOS	May allow an authenticated, physical attacker to bypass secondary authentication and access an affected macOS device.	Authentication Bypass	This vulnerability affects Cisco Duo Two-Factor Authentication for macOS.	MEDIUM	CVE-2023-20199
Cisco SD-WAN Software	May allow an authenticated, local attacker to access sensitive information.	Information Disclosure	This vulnerability affects the following Cisco products if they were running a vulnerable release of Cisco SD-WAN Software: • SD-WAN vBond Orchestrator Software • SD-WAN vEdge Cloud Routers • SD-WAN vEdge Routers • SD-WAN vManage Software • SD-WAN vSmart Controller Software	MEDIUM	CVE-2021-1546

Cisco Small Business 200, 300, and 500 Series Switches	May allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface on an affected device.	Stored Cross-Site Scripting (XSS)	This vulnerability affected the following Cisco products: • Small Business 200 Series Smart Switches • Small Business 300 Series Managed Switches • Small Business 500 Series Stackable Managed Switches	MEDIUM	CVE-2023-20188
Cisco Unified Communications Manager	May allow an authenticated, remote attacker to cause a denial of service (DoS) condition on an affected device.	Denial of Service (DoS)	This vulnerability affected Cisco Unified CM and Unified CM SME.T	MEDIUM	CVE-2023-20116
Cisco Secure Workload	May allow an authenticated, remote attacker with the privileges of a read-only user to execute operations that should require Administrator privileges. The attacker would need valid user credentials.	Privilege Escalation	This vulnerability affected Cisco Secure Workload with the default configuration.	MEDIUM	CVE-2023-20136

These vulnerabilities are rated from **CRITICAL** to **MEDIUM** risks. Software patches exists to address these risks.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

Please notify VRM with any questions or concerns you may have.

References

- Cisco Security Advisories